AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

District of Vermont

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
TWO CELLULAR TELEPHONES, A BLACK LG CELL PHONE WITH CRACKED SCREEN, AND A BLACK AT&T CELL PHONE, IN THE CUSTODY OF THE UNIVERSITY OF VERMONT POLICE DEPARTMENT

Case No. 2:20-mj-128

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A.

located in the _____ District of Vermont, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 2113(b)	Bank larceny in excess of $1,000

The application is based on these facts:

See Affidavit, incorporated herein.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

SA Colin Simons, FBI
Printed name and title

Sworn to before me and signed in my presence.

Date: 10/28/2020

Judge's signature

City and state: Burlington, VT

Hon. John M. Conroy, U.S. Magistrate Judge
Printed name and title

ATTACHMENT A

The property to be searched (the Electronic Devices) are two Smart Phones seized by law enforcement on October 8, 2020 and currently stored at the University of Vermont Police Department in Burlington, Vermont:

- **black LG cell phone with cracked screen, and**
- **black AT&T cell phone**

(collectively, the "Electronic Devices").

ATTACHMENT B

All data on the Electronic Devices described in Attachment A that constitutes evidence of violations of 18 U.S.C. § 2113(b), including:

a. Photographs and other images of currency, receipts, purchases, vehicles, and/or locations;

b. Communications related to identifying locations, surveillance, planning or executing thefts, and sharing proceeds—including e-mails, text messages, instant messages, chat logs, attachments to messages, and drafts;

c. Ledgers, notes, or other financial records of types, as well as information about the dates and places of those transactions;

d. Records of financial transactions, including wire transfers, bank deposits and withdrawals, credit or debit card activities, and electronic currency activities;

e. Lists of locations, associates and co-conspirators, including identifying and contact information;

f. Contact lists showing names, street names, nicknames, phone numbers, email addresses, screen names of associated individuals;

g. Geographic locations of the Electronic Devices at times relevant to the investigation;

h. Records of travel, including ticketing information, rental agreements, and hotel reservations and payments;

i. Evidence indicating how and when the cellular device and associated cellular service was used to determine the chronological context of cellular device use, account access, and events relating to the crime under investigation;

j. Evidence of user attribution showing who used or owned the cellular device at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, usernames and passwords, documents, and browsing history;

k. Records evidencing the use of the Electronic Devices to access the internet, including:

a. Internet Protocol addresses used;

b. Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, Colin Simons, having been first duly sworn, do hereby depose and state as follows:

Affidavit Purpose and Affiant Background

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of two cellular telephones,

- **black LG cell phone with cracked screen, and**
- **black AT&T cell phone**

(collectively, the "Electronic Devices") which are described with particularity in Attachment A and are currently stored in evidence at the University of Vermont Police Department (UVMPD), and the extraction from the Electronic Devices of the electronically stored information described in Attachment B.

2. I am a Special Agent with the Federal Bureau of Investigation (FBI) currently assigned to the Rutland, Vermont Resident Agency of the Albany, New York Division. I have been a Special Agent for over 15 years. I am responsible for investigating a variety of criminal violations, to include robberies and thefts from financial institutions. As a Special Agent, I am authorized to investigate violation of laws of the United States and to execute warrants issued under the authority of the United States.

3. Based on my training and experience I know the following:

a. Persons who participate in larcenies with other individuals frequently use cellular telephones and other electronic devices to coordinate their unlawful activities and to maintain contact with their co-conspirators.

b. I know that information stored in the memories of these communications devices often constitutes evidence of conspiracy as well as the movement and disposition of currency representing the proceeds of the larcenies. Among other things, the evidence may contain the telephone numbers assigned to the communication devices, messages received by or sent from the devices, identification numbers and other information contained in their

electronic memories, and the records of telephone numbers to which communications were sent and from which communications were received.

c. Using their cellular telephones, individuals often take photographs or videos while doing surveillance of potential locations being targeted, cash from thefts, assets obtained from stolen proceeds, and other evidence pertaining to the crimes.

d. I also know that persons engaged in such illegal activities will often deny ownership of these phones in an attempt to thwart law enforcement's efforts to connect them to the crimes under investigation, as well as to co-conspirators and other potential locations being targeted.

e. Data contained in cellular telephones may reveal the physical location of the cellular phone at various times. For example, the camera embedded on the phone may record its latitude and longitude at the time it takes a photograph and record that location in the metadata associated with the picture. Also, if a cellular phone has Global Positioning System ("GPS") capabilities (which many do), additional information regarding locations of the phone, while it follows GPS directions, may be recovered from the device.

4. Based on the facts set forth in this affidavit, there is probable cause to believe that evidence of crimes committed by Matthew MORGAN and others known and unknown to law enforcement—specifically, stealing bank property having a value in excess of $1000, in violation of 18 U.S.C. § 2113(b)—is located on the Electronic Devices. The Electronic Devices were seized by law enforcement on October 8, 2020, and they are currently stored at UVMPD.

5. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from reviewing investigative reports, and from conversations with UVMPD personnel, including Sgt. Jim Phelps. I have reviewed reports made available by other law enforcement authorities and have had discussions with other law enforcement officers investigating this matter who have interviewed witnesses.

6. Because this affidavit is submitted for the limited purpose of establishing probable cause for a search warrant, I have not set forth each and every fact learned during the course of the

investigation.

PROBABLE CAUSE

7. On September 22, 2020, UVMPD was dispatched to the University of Vermont Dudley Davis Center, 590 Main Street, Burlington, Vermont for a possible theft. The caller, Richard Barry, advised he was on the first floor of the Davis Center and that a Citizens Bank ATM kiosk was missing from its assigned position in the Davis Center tunnel.

8. On September 21, 2020, Barry received an email from a representative of PAI New England requesting that he check on the ATM. PAI New England was responsible for monitoring leased ATM kiosks at various locations in New England including the Citizens Bank ATM at the Davis Center. PAI New England had noticed a decrease in use of the ATM and asked Barry if the unit was still accessible.

9. On September 22, 2020, Barry walked down to the Davis Center tunnel where the Citizens Bank ATM was supposed to be located. When he arrived there, he found the ATM missing so he emailed PAI New England to let them know the unit was not there.

10. Sgt. Phelps spoke with PAI New England and learned the ATM was last used by a customer on September 12, 2020 at 4:50 p.m. and the unit would have had $23,100 remaining in the machine at the time it was removed from the Davis Center. According to Loomis Armored Car Service, which services the Citizens Bank ATM, they typically only put $20 bills in the ATM kiosks.

11. UVMPD reviewed the Davis Center CCTV security camera footage. Surveillance footage showed two males removing the ATM from the Davis Center on September 12, 2020 shortly after 9:00 p.m. One individual was not wearing anything to conceal or cover his face and the other person was wearing what appeared to be a facemask.

12. When Phelps watched the security camera footage, he observed two males enter the

breezeway to the Davis Center tunnel on the south side of Main Street. The two males walked down the stairs into the Davis Tunnel. One pulled a red hand truck and they arrived a short time later at the Citizens Bank ATM. The ATM was eventually loaded onto the hand truck and the two men then walked towards the main lobby of the Davis Center and out the northwest doors with the ATM. Before the ATM was taken, the top of the unit was covered with a white sheet. The individual later identified as Ruebin Beard did not have any face covering. The individual later identified as MORGAN had what appeared to be a facemask obscuring his face. UVMPD also observed MORGAN appear to use a cell phone while in the tunnel.

13. Images of the two individuals were shared with UVMPD's law enforcement contacts in an attempt to identify them. Burlington Probation and Parole contacted UVMPD advising the first male was a Ruebin Beard. Probation Officer Brandon Bushey recognized Beard as Bushey previously worked in a correctional center in 2009 to 2010 when Beard was being housed there.

14. On October 2, 2020, Burlington Police Det. Sgt. My Nguyen contacted UVMPD to advise that he may have identified the second person in the ATM theft. Nguyen reported that he noticed Matthew Morgan's Facebook page had updated its profile picture on September 13, 2020. The updated picture depicted a large stack of money. When viewing the Facebook page of MORGAN, UVMPD identified the Facebook user ID for the page as Matt.Morgan.3720. Phelps looked at MORGAN's Facebook account and saw what appeared to be stacks of money. The visible bills were all $20 bills. Under the friends section of MORGAN's Facebook account was Ruebin Beard's Facebook account. Phelps was able to positively ID the individual in the profile picture of MORGAN's Facebook page as MORGAN from his review of images of MORGAN from a law enforcement database.

15. On October 5, 2020, Phelps made phone contact with Officer Jonathan Teske from the

Vermont Department of Corrections. In September 2020, MORGAN was on furlough from a lengthy prison sentence imposed in Vermont for a series of burglaries. While on furlough, MORGAN was required to wear a bracelet-like device that had GPS location monitoring capabilities. DOC contracted with a company named Attenti to monitor the location of its furloughees. Teske explained that the GPS device recorded MORGAN's exact location, with latitude and longitude coordinates, about every 60 seconds.

16. Investigators have obtained from Attenti a compilation of MORGAN's whereabouts, as established by GPS data, beginning at midnight on September 12, 2020 and continuing through midnight ending September 14. This GPS data shows that at about 9 p.m. on September 12, 2020, MORGAN was on the UVM campus in or in close proximity to the Davis Center. The data also shows that at 1:17 a.m. on September 13, MORGAN went to 1078 Avenue D in Williston and remained there for about 15 minutes. He then departed the immediate area but returned to 1078 Avenue D at about 1:48 a.m. MORGAN stayed at that location for another 20 minutes.

17. On October 6, 2020, Phelps traveled to 1078 Avenue D in Williston, which is an empty trucking terminal located at the far north end of the park. He drove into the parking lot on the southeast end of the building and got out of the car to check for any sign of the ATM.

18. Phelps noticed at the east end of the parking lot a steep embankment, which had a guard rail along most of the embankment. At the southeast end of the railing the traffic barrier ended and the area to the steep bank was wide open. While walking in that direction, he noticed a piece of gray plastic approximately 3 inches long on the tarmac. As he got closer to the southeast corner of the lot, he noticed a broken black handle similar to what Phelps has seen in the past on ATMs. UVMPD Det. Denise D'Andrea, who was with Phelps, was standing at the end of the guardrail looking over the steep dirt embankment when she found the ATM on its side approximately 30 feet down the bank.

The ATM was recovered and the scene processed. Approximately 20 feet from the ATM were two ATM cash cassettes that money would have been stored in. Each of the cassettes had its door torn off. The doors were located in the general vicinity of the cassettes.

19. On October 7, 2020, Phelps learned that Det. Dale Crispin of the South Burlington, Vermont Police Department was investigating MORGAN for a burglary on September 12, 2020 at 2:40 p.m. In that case, several wallets were taken from a place of business and the stolen credit cards were used at a number of locations. Phelps observed surveillance images captured during the burglary being investigated by Det. Crispin. The suspect entered what appeared to be a break room wearing the same clothes as the person who came to the Davis Center and bent down to unplug the ATM machine. The person wore blue jeans, a pull-over fleece-like jacket, a Boston Red Sox cap and sneakers.

20. On October 8, 2020, the Burlington, Vermont Police Department (BPD) took MORGAN into custody on a separate investigation. MORGAN was in possession of a black Jeep Patriot bearing Vermont temporary registration D15737 / VIN: 1JNF1GB6BD156857. The vehicle was seized and eventually brought to UVMPD. During his arrest, MORGAN asked BPD officers to retrieve his phone for him from the inside of the car. BPD officers located and seized a black AT&T cell phone from the vehicle.

21. On October 8, 2020, Phelps assisted in the execution of a state search warrant on MORGAN's North Star Motel room. Located during the search were a dark pair of pants and dark shirt that appeared to match the clothing MORGAN wore during the ATM larceny. During the search, a black LG cell phone with a cracked front screen was located and seized by officers.

22. On October 12, 2020, Phelps met with the staff at Carter Cars located at 1089 Shelburne Road, South Burlington, Vermont. Carter Cars staff confirmed on September 14, 2020, they sold a

black 2011 Jeep Patriot to MORGAN. Carter Cars records included a photocopy of MORGAN's state identification card issued through the Vermont Department of Human Services and showed the total purchase price of the vehicle to be $6,785.82, which was paid in full. MORGAN put down $2,785.82 in cash plus three different transactions from MORGAN's ATM /Debit card of $1,998.51, $2,000 and $1.49. The primary sales person for the sale remembered the transaction because MORGAN counted out the money for his cash portion of the transaction in what appeared to be new crisp $20 bills.

23. On October 13, 2020, UVMPD executed a state search warrant on the seized Jeep Patriot. Among the items located during the search were a pry bar and light weight hammer. Sgt. Phelps compared the claws on the pry bar to forced-entry marks on the recovered ATM cabinet. In Phelps' lay opinion, the pry marks on the ATM cabinet appeared to match up with claws on the bar.

24. Andrew Carpenter, an employee with the Loss Prevention Group of Citizens Bank, reports that on September 12, 2020, Citizens Bank had its deposits insured by the Federal Deposit Insurance Corporation.

25. Based on my training and experience in thefts of financial institutions, I know that:

a. Individuals who engage in such activities are capable of amassing tens of thousands of dollars or more in a short periods and often physically retain such currency for long periods, even after their illicit activity has ceased;

b. It is common for individuals to put bank accounts, assets, and cell phones in the names of associates, family members, or fictitious names to avoid detection and to conceal illegitimate income;

c. Individuals maintain and access books, records, receipts, bills of sale, notes, computer software, airline tickets, money orders, and other documents relating to their proceeds, and much of this information is commonly stored electronically on cellular telephones and other electronic devices capable of storing electronic data;

d. Individuals commonly maintain names and contact information in books, ledgers, computers, cellular telephones, other electronic devices, and digital storage media,

which reflect the names, nicknames, screen names, addresses, telephone numbers, and email addresses of their co-conspirators;

e. Persons involved in thefts and robberies keep and access electronic records of the storage, purchase, and/or trading of currency, digital currency, financial instruments (including stocks, bonds, certificates of deposit, etc.), precious metals, jewelry, automobile titles, and other items of value, and those records can constitute evidence of financial transactions relating to the concealment of the source of large sums of money, whether in the form of notes, receipts, bank statements, check registers, financial account statements, wire transfer records, and documentation of foreign bank accounts; these records are often stored inside their cellular telephones;

f. Individuals involved in thefts and robberies amass proceeds from their activities and they often attempt to legitimize ("launder") the proceeds using domestic and foreign banks, casinos, brokerage houses, real estate firms, shell corporations, business fronts, or other financial institutions with their attendant services, including sales of securities, cashier checks, money drafts, money orders, wire transfers, and letters of credit; evidence of laundering attempts is commonly found within the electronic storage of their cellular telephones long after they cease criminal activity;

g. Persons engaged in criminal activity often spend the proceeds of their criminal activity and maintain or access records of their expenditures on their cellular telephones, long after their criminal activity has ceased—specifically, these records may include:

i. Records of income and expenses, such as profit and loss statements and income and expense journals that reflect the expenditure of the proceeds;

ii. Evidence of the expenditure of the proceeds or purchase of assets with the proceeds, such as invoices, receipts, rental statements, lease statements, travel records, earnest money agreements, escrow statements, and real estate deeds;

iii. Records of the accumulation of assets acquired with the proceeds of criminal activity, such as ledgers, balance sheets and financial statements, reflecting both assets and liabilities;

iv. Checking and savings account records consisting of monthly statements, duplicate deposit slips, and canceled checks reflecting the deposit and disbursement of proceeds;

v. Contracts and other agreements reflecting associates between individuals relative to business ventures;

vi. Images or other records of cashier's checks, money orders, and wire transfers involving the proceeds of criminal activity; and

vii. Photographs of their associates, their property, surveillance of target locations, including photographs of currency and purchases constituting documentation of unexplained wealth that is consistent with trafficking in controlled substances.

26. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. Cellular telephone: A cellular telephone (or mobile telephone, or wireless telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A cellular telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, cellular telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Electronic Devices may also include global positioning system ("GPS") technology for determining the location of the device.

b. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication device and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system ("GPS") technology for determining the location of the device. PDAs also often contain digital cameras.

c. Smart Phone: Smart phone is a term typically used to refer to a cellular telephone that has combined the capabilities of a cellular telephone and a typical PDA.

d. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

e. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records of the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated "GPS") consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

f. IP Address: An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

g. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between Device on the Internet often cross state and international borders, even when the Device communicating with each other are in the same state.

27. Based on my training and experience, I know the Electronic Devices listed in Attachment A are Smart Phones and include the features outlined above.

a. Based on my knowledge, training, experience, and discussions with other law enforcement officers, I know that digital files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer or smart phone, the data contained in the file do not actually disappear; rather, those data remain on the device's storage medium until they are overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by and active file—for long periods before they are overwritten. In addition, a device's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media contain electronic evidence of how a computer has been used, what it has been used for, and who has used it (user attribution). To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Device users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into temporary Internet directory or "cache."

28. As further described in Attachment B, this application seeks permission to locate not only digital files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how the Electronic Devices were used, the purpose of their use, who used them, and when. There is probable cause to believe this forensic electronic evidence will be on the Electronic Devices for the following reasons:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the

attachment of peripherals, the attachment of USB flash storage Device or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created, and the sequence in which they were created, although this information can later be falsified.

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus spyware and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicting when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a cellular telephone works can, after examining this forensic evidence in its proper context, draw conclusions about how a cellular telephone was used, the purpose of its use, who used it, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a cellular telephone was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

Conclusion and Requests

29. Based on the facts set forth in this affidavit, there is probable cause to believe that evidence of crimes—specifically, violation of 18 U.S.C. §§ 2113(b)—committed by MORGAN, and others known and unknown to law enforcement, will be located in the Electronic Devices. Accordingly, I respectfully request the Court issue the Search Warrant authorizing the search of the Electronic Devices described in Attachment A and the seizure of the data described in Attachment B.

30. Because this warrant seeks only permission to examine devices already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

Dated at Burlington, in the District of Vermont, this 28th day of October, 2020.

Colin M. Simons, Special Agent
Federal Bureau of Investigation

Sworn to and subscribed before me this 28th day of October, 2020.

John M. Conroy, Magistrate Judge
United States District Court
District of Vermont